Chef C h i

Berlin, 21.November 1944

Niederschrift der Besprechung über
Chiffrierfragen - 15.11.44

Chef Ag WNV, Gen.Lt. G i m m l e r , begrüßt die Vertreter der Dienststellen und macht folgende Ausführungen:

In der 1. Chi-Besprechung sind Fragen der Organisation und des Einsatzes besprochen worden. In der 2. Chi-Besprechung haben die Spezialisten das Wort. Es werden heute nur Fragen des Geheimschriftwesens erörtert werden.

Aus der 1. Chi-Besprechung müssen nochmals zwei Punkte erwähnt werden:

1. Die von Chi gegebenen Gutachten behalten so lange Gültigkeit, bis sie durch neue Gutachten von Chi außer Kraft gesetzt werden.
2. Nach dem Keitel-Befehl muß Chi vor Einführung einer neuen Geheimschrift um Zustimmung befragt werden. Die Entscheidung über die Einführung bleibt den Wehrmachtteilen vorbehalten. Es wird jedoch den Wehrmachtteilen empfohlen, die Gutachten von Chi weitgehendst zu berücksichtigen.

Die heutigen 4 Vorträge spiegeln die Aufgaben und die Neugliederung auf dem Gebiet der Geheimschriften von Chi wider.

1. Vortrag: Sdf. Dr.Fricke:

Stand der Entwicklung eigener Heeres-Geheimschriften; Methoden der Schlüsselherstellung.

I. Notwendige Voraussetzungen für eine erfolgreiche Entwicklung der eigenen Verfahren sind:

1.) Forschung an eigenen und fremden Chiffrier-Verfahren,

2.) Nutzbarmachung der Erfahrungen bei der praktischen Entzifferung.

Die Entwicklung von Geheimschriftverfahren im Laufe der letzten Jahre ist im wesentlichen bestimmt worden:

1.) durch besonders intensive Forschung (zum Teil erstmalige Forschungsarbeiten), die naturgemäss zu Änderungen der Verfahren geführt hat,

2.) durch die wechselnden Forderungen der Truppe.

II. Zur Charakterisierung des augenblicklichen Standes der Entwicklung von Chiffrierverfahren und der Methoden der Schlüsselherstellung wurden folgende Beispiele gegeben:

1.) Untersuchungen werden durchgeführt, um auf der Basis der heutigen Funktafelverfahren ein Chiffrierverfahren für vorderste Verbände (Truppennachrichtenverbände, Boden-Bordverkehr, kleine Küstenfahrzeuge) zu schaffen.

2.) Untersuchungen an Notschlüsselverfahren werden durchgeführt. Notschlüssel für Hand- und Maschinenschlüssel sollen eingeführt werden.

3.)

Die Sicherheitsbeurteilung einer Geheimschrift ist abhängig vom Stand der eigenen Entzifferung und den Fortschritten der Theorie. Endgültig sind nur negative Urteile; positive Urteile können abgeändert werden. wenn neue Erkenntnisse und Erfahrungen gewonnen sind.

Zur Sicherheitsbeurteilung muß untersucht werden,

1. ob der Variationsbereich der Schlüsselunterlagen genügend groß ist,
2. ob Klartexteigentümlichkeiten, die zur Lösung führen können, verdeckt werden,
3. ob besondere Gesetzmäßigkeiten, die unbefugte Lösungen begünstigen können, vermieden sind,
4. ob die Geheimschrift kompromißsicher ist.

Die Überprüfung der in der Wehrmacht eingeführten Verfahren und Schlüsselmaschinen zeigt, daß alle strengen Sicherheitsforderungen nicht immer erfüllt sind. Ein großer Teil der eigenen Verfahren ist nicht kompromißsicher. Es wurde angegeben, wo Kompromisse auftreten können und welche Einbruchsmöglichkeiten sich hieraus im einzelnen ergeben. Die praktische Sicherheit der eigenen Verfahren hängt in besonderem Maße von der Einhaltung der Vorschriften und der Vermeidung von Schlüsselfehlern ab. Das neuentwickelte Gleichlaufverfahren, das mit dem neuen Schlüsselzusatz 42 c gekoppelt werden soll, sowie das Schlüsselgerät 39 stellen vom Sicherheitsstandpunkt wesentliche Fortschritte dar.

Die einzige Geheimschrift, deren absolute E-Festigkeit bewiesen werden kann, ist der individuelle Zahlenwurm. Seine Anwendungsmöglichkeit ist jedoch beschränkt.

Zu diesem Vortrag führt Gen.Lt. Gimmler aus:

Während der Entwickler bei Chi, Dr. Fricke, mit zwei Stellen, nämlich Wehrmacht und Heer zusammenarbeiten muß, arbeitet der Prüfer bei Chi, Lt. Dr. Stein, mit vier Stellen, nämlich Wehrmacht, Heer, Marine und Luftwaffe zusammen.

Chi spricht die Bitte aus, daß Marine und Luftwaffe alle Geheimschriften zur Sicherheitsüberprüfung an Chi geben.

Major Lechner: Ist ein Rasterkompromiß lösbar?

Lt.Dr. Stein: Ein Klar-Geheim-Kompromiß beim Raster führt zur Rekonstruktion der Lösung und desrbenutzten Teiles des Rasterfeldes und erleichtert den weiteren Einbruch.

3. Vortrag: Reg.Rat Dr. Hüttenhain:

Entzifferung fremder Geheimschriften.

Die Entzifferung fremder Geheimschriften vollzieht sich in zwei Schritten:

1. Erkennen, welche Geheimschrift vorliegt,
2. Lösen der Geheimschrift, d.h. Umwandlung der Geheimtexte in Klartexte.

Der Entzifferer muß alle in der Praxis aufgetretenen Geheimschriften kennen. Die Anzahl dieser Geheimschriften ist sehr groß; es existiert jedoch nur eine beschränkte Anzahl verschiedener Grundtypen. Der Entzifferer muß ferner über gute Sprachkenntnisse, mathematische Kenntnisse, Fingerspitzengefühl, Ausdauer, Verschwiegenheit und vor allem Erfahrung verfügen.

1. Welche Geheimschrift liegt vor?

Alle aufgenommenen Sprüche werden genau registriert (aufgelistet), um Kenngruppen bzw. Spruchschlüssel zu erkennen, schlüsselgleiches Material zusammenzulegen und nach Kompromissen zu suchen.

Dann wird eine genaue Analyse der Geheimtexte gemacht; es werden Statistiken angefertigt: Häufigkeiten, Wiederholungen, Parallelstellen, ev. auftretende Phasen.

Kompromisse und Statistiken liefern also die Mittel, um eine Geheimschrift zu bestimmen. Dabei ist die Kenntnis von der Entwicklung des Geheimschriftwesens des betr. Landes für den Entzifferer von großer Bedeutung.

2. Lösen einer Geheimschrift:

Alle Grundverfahren werden vom Sprachler gelöst.

Bei den Überschlüsselungen müssen zwei verschiedene Lösungsmöglichkeiten unterschieden werden:

a) Statistische Lösung,

b) Kompromißlösung.

An Hand von Lichtbildern wurde gezeigt, wie eine allgemein verbreitete Geheimschrift durch fehlerhafte Anwendung (längere Parallelstellen, Sammelsprüche bzw. ungenügende Klartextabänderungen bei Spruchwiederholungen) bloßgestellt und gelöst worden ist.

Die Entzifferung fremder Geheimschriften, deren Bedeutung für die Staats- und Kriegführung sowie für die Sicherheitsbeurteilung der eigenen Geheimschriften offensichtlich ist, wird in Zukunft nur dann leistungsfähig sein, wenn sie maschinelle Hilfsmittel einsetzt.

Zu diesem Vortrag führt Gen.Lt. Gimmler aus:

Der Entzifferer soll dem Überprüfer Anregungen geben. Durch die Organisation bei Chi ist sichergestellt, daß die Erkenntnisse der Entzifferung dem Überprüfer zur Kenntnis gelangen. Über den Überprüfer kommen alle Erkenntnisse der Entzifferung auch den Wehrmachtteilen zugute.

4. Vortrag: Reg.Baurat Dipl.-Ing. Rotscheidt:

Vorführung von Entzifferungshilfsgeräten.

Vor der Vorführung der von Chi entwickelten und gebauten E-Hilfsgeräte wurde ein allgemeiner Überblick gegeben:

Die Entzifferung fremder und die Überprüfung der Sicherheit eigener Geheimschriften erfordern einen immer grösser werdenden Einsatz von Arbeitskräften und Zeit. Es be-

stellt

steht daher die Notwendigkeit, geeignete Geräte und Maschinen einzusetzen, um Arbeitskräfte und Zeit einzusparen. Außerdem erfolgt die Maschinenauswertung fehlerfrei.

Die Entzifferung verwendet von vorhandenen Maschinen normale Rechenmaschinen und Lochkartenmaschinen (Hollerith). Da mit diesen Maschinen jedoch bei weitem nicht alle Probleme mit Erfolg bearbeitet werden können, besteht die Notwendigkeit, spezielle Geräte herzustellen.

Diese Geräte können in handbediente und automatisch arbeitende Geräte eingeteilt werden. Im allgemeinen besteht jedes Gerät aus 3 Teilen, dem Abtastgerät, der Recheneinrichtung und dem Registrierwerk.

Die Entwicklung der Geräte erfolgt in engster Zusammenarbeit mit den Spezialisten der betr. Sachgebiete; es wird stets auf universelle Verwendbarkeit geachtet. Für die Fertigung stehen zwei eigene Werkstätten zur Verfügung.

Die Weiterentwicklung der Geräte zielt auf schnellaufende Maschinen hin, um große Materialmengen in kürzester Zeit verarbeiten zu können.

An diese Ausführungen schloß sich die Besichtigung der Geräte an.

Im Anschluß an die Vorführung der E-Hilfsgeräte gibt Gen.Lt. Gimmler bekannt, daß in ca. 8 Wochen die nächste Chi-Besprechung stattfinden wird. Thema: Sprachverschlüsselung.

Berlin, 15.11.1944

NV/Chi

Anwesenheitsliste

Chef Ag WNV	Gimmler, Gen.Lt.
OKH/Chef HNW/IV	Binder, Major
	Ruppel, Oblt.
/LNA	Lechner, Major
/Wa Prüf 7 III	Liebknecht, Dr.-Ing.
IV	Lotze, Dr.-Ing.
OKM 4./Skl II	Lucan, Kpt.z.S.
	Singer, Freg.Kpt.
III	Tranow, Ob.Reg.Rat
	Schwabe, Amtsrat
6./Skl III	Stiehler, Dr.,Reg.Rat
	Reimers, Dr., Reg.Rat
OKL/Gen Nafue 2	Schultze, Dr., Obstlt.
	Blumberg, Major
3	Hoheisel, Prof.Dr.,Reg.Baurat
	Porth, Hptm.
/Chef WD	Wüsthoff, Dr., Reg.Rat
	Naumann, Ob.Insp.
Reichsführer SS/Chef FMW	Weber, Obstlt.
	Kusik, SS-Hschf.
MB IV	May, Hptm.
Ag WNV/GBN	Sobe, Sturmbannf.
/Fu	Mushake, Hptm.
Chef Chi	Kettler, Oberst
Chi A	Mettig, Major
	Fricke, Dr., Sdf.(Z)
B	Fenner, Min.Rat
	Hüttenhain, Dr., Reg.Rat
	Rotscheidt, Dipl.-Ing.Reg.Baurat
	Stein, Dr., Lt.